

ABSTRACT OF THE DISCLOSURE

5 A method and system for efficiently conducting secure communications
in a commuter network are provided. Secure communications in a network are
typically of the Secure Socket Layer ("SSL") and Transport Layer Security
("TLS") formats. These formats require the server to decrypt numerous
encrypted messages at the cost of efficiency and speed. By combining the
10 encrypted messages into a batch and utilizing a Rivest-Shamir-Adleman
("RSA") batch decryption algorithm, the efficiency of the decryption is
improved. Methods for improving this process include replacing the required
number of divisions and inversion with more efficient multiplication operations.
Further computation savings are realized by reducing the number of
15 exponentiations and structuring the batches of encrypted messages to contain
balanced exponents.